JP2001507528(A)

ROOT KEY COMPROMISE RECOVERY

Publication number: JP2001507528 (T)
Publication date: 2001-06-05
Inventor(s):
Applicant(s):
Classification:
- international: *H04L9/08; H04L9/30;* H04L9/08; H04L9/28; (IPC1-7): H04L9/08
- European: H04L9/08; H04L9/30
Application number: JP19970515331T 19961114
Priority number(s): US19950555697 19951114; WO1996US18037 19961114

Abstract not available for JP 2001507528 (T)
Abstract of corresponding document: **WO 9718655 (A1)**

A method of recovering from a compromise of a root key which is the private key of a first public key-private key pair, the method including the steps of electronically sending out an emergency message (10) indicating that the root key has been compromised and also containing a replacement key (16) and a digital signature (22) which was generated by using the root key; and publishing in an out-of-band channel a value V, wherein V is derived from the emergency message.

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号
特表2001－507528
（P2001－507528A）
(43)公表日　平成13年６月５日(2001.6.5)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ
			６０１Ｆ

審査請求　有　　予備審査請求　有　（全 22 頁）

(21)出願番号　特願平9－515331
(86)(22)出願日　平成８年11月14日(1996.11.14)
(85)翻訳文提出日　平成10年４月14日(1998.4.14)
(86)国際出願番号　ＰＣＴ／ＵＳ９６／１８０３７
(87)国際公開番号　ＷＯ９７／１８６５５
(87)国際公開日　平成９年５月22日(1997.5.22)
(31)優先権主張番号　０８／５５５，６９７
(32)優先日　平成７年11月14日(1995.11.14)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＡＵ，ＣＡ，ＪＰ

(71)出願人　マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　98052　レッドモンド　マイクロソフト　ウェイ　ワン
(72)発明者　スペルマン　ジェフリー　エフ
アメリカ合衆国　ワシントン州　98019　デュバル　エヌ　イー　ミラー　26705
(72)発明者　トムリンソン　マシュー　ダブリュー
アメリカ合衆国　ワシントン州　98006　ベルブー　Ｎｏ．１－201　エス　イー　ニューポート　ウェイ　13158
(74)代理人　弁理士　開口　宗昭

(54)【発明の名称】　ルート・キーが危機にさらされた時の回復

(57)【要約】
第一の公開鍵と秘密鍵のペアの秘密鍵であるルート・キーを危機にさらされた状態から回復させる方法である。その方法は、ルート・キーが危機にさらされたことの通知と、置き換えの鍵と、ルート・キーを使って生成したデジタル署名を含む緊急メッセージを送信する手順と、緊急メッセージから導き出される変数Ｖをアウト・オブ・チャネルを経由して入手する手順とから成る。

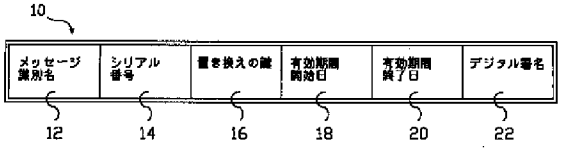

図1

【特許請求の範囲】
１．ルート・キーの置き換え方法であって、前記ルート・キーが第一の公開鍵と秘密鍵のペアの秘密鍵であり、
前記方法が、
電気的手段によりメッセージを送る手順であって前記メッセージがルート・キーの置き換えを行うという通知であり置き換えの鍵とルート・キーを使って生成されたデジタル署名を含むメッセージであって
前記置き換えの鍵が第一の公開鍵と秘密鍵のペアと取り替える第二の公開鍵と秘密鍵のペアの公開鍵であるメッセージを送る手順と、
通常の通信では使用されないアウト・オブ・バンド・チャネルでメッセージから導き出せるＶを発行する手順
とからなることを特徴とするルート・キーの置き換え方法。
２．メッセージの少なくとも一部分に一方向関数を適用して前記Ｖを算出することを特徴とする請求の範囲１に記載のルート・キーの置き換え方法。
３．置き換えの鍵と識別名を結合して生成されるメッセージであって
前記識別名はメッセージが置き換えの鍵を配送することを示しているメッセージを生成することを特徴とする請求の範囲２に記載のルート・キーの置き換え方法。
４．置き換えの鍵とシリアル番号を結合して生成されるメッセージであって前記シリアル番号は多数のルート・キーのうちのどれを置き換えるかを示しているメッセージを生成することを特徴とする請求の範囲２に記載のルート・キーの置き換え方法。
５．置き換えの鍵と置き換えの鍵がいつ失効するかを示す有効期間終了日とを結合してメッセージを生成することを特徴とする請求の範囲２に記載のルート・キーの置き換え方法。

６．置き換えの鍵と置き換えの鍵が有効となる期日を示す有効期間開始日とを結合してメッセージを生成することを特徴とする請求の範囲２に記載のルート・キーの置き換え方法。

７．ルート・キーの置き換え方法であって、
前記ルート・キーが第一の公開鍵と秘密鍵のペアの秘密鍵であり、
前記方法が、
置き換えの鍵とルート・キーの置き換えを行うという通知を含む第一のメッセージを生成する手順であって
前記置き換えの鍵は第一の公開鍵と秘密鍵のペアと取り替える第二の公開鍵と秘密鍵のペアの公開鍵であるメッセージを生成する手順と、
第一のメッセージにルート・キーを使ってデジタル署名を生成する手順と、
第二のメッセージを生成するため第一のメッセージとデジタル署名を結合する手順と、
第二のメッセージを電気的手段により送信する手順と、
アウト・オブ・バンド・チャネルを使って第二のメッセージから導き出されるＶを発行する手順とから成ることを特徴とするルート・キーの置き換え方法。
８．ルート・キーの変更に応ずる方法であって、
前記ルート・キーが第一の公開鍵と秘密鍵のペアの秘密鍵であり、
前記方法が、
メッセージを電気的手段によって受信する手順であって
前記メッセージがルート・キーの置き換えを行うという通知であり
置き換えの鍵とルート・キーを使って生成されたデジタル署名を含むメッセージであって
前記置き換えの鍵が第一の公開鍵と秘密鍵のペアと取り替える第二の公開鍵と秘密鍵のペアの公開鍵であるメッセージを受信する手順と、
メッセージのデジタル署名を照合するためルート・キーの対応した公開鍵を使用する手順と、
アウト・オブ・バンド・チャネルを通してメッセージの少なくとも一部にアルゴリズムを適用してメッセージから導き出せるＶを入手する手順と、
前記メッセージの少なくとも一部にアルゴリズムを作用させて得られるＢを生成するためにアルゴリズムを適用する手順と、

ＢとＶを比較する手順と、
ＢとＶが一致した場合にルート・キーに対応した公開鍵を置き換えの鍵と取り替える手順とから成ることを特徴とするルート・キーの変更に応ずる方法。
９．ルート・キーを危機にさらされた状態から回復させる方法であって、
前記ルート・キーが第一の公開鍵と秘密鍵のペアの秘密鍵であり、
前記方法が、
電気的手段により緊急メッセージを送る手順であって
前記緊急メッセージはルート・キーが危機にさらされたという通知であり
置き換えの鍵とルート・キーを使って生成されたデジタル署名を含み
前記置き換えの鍵は第一の公開鍵と秘密鍵のペアと取り替える第二の公開鍵と秘密鍵のペアの公開鍵である緊急メッセージを送る手順と、
アウト・オフ・チャネルで緊急メッセージから導き出せるＶを発行する手順とから成ることを特徴とするルート・キーを危機にさらされた状態から回復させる方法。
１０．ルート・キーを危機にさらされた状態から回復させる方法であって、
前記ルート・キーが第一の公開鍵と秘密鍵のペアの秘密鍵であり、
前記方法が、
電気的手段により緊急メッセージを受信する手順であって
前記緊急メッセージはルート・キーを置き換えるという通知であり
置き喚えの鍵とルート・キーを使って生成されたデジタル署名を合み
前記置き換えの鍵は第一の公開鍵と秘密鍵のペアと取り替える第二の公開鍵と秘密鍵のペアの公開鍵である緊急メッセージを受信する手順と、

緊急メッセージのデジタル署名を照合するため前記第一の公開鍵と秘密鍵のペアの公開鍵を使用する手順と、
アウト・オブ・バンド・チャネルを通してメッセージの少なくとも一部に
アルゴリズムを作用させてメッセージから導き出せるＶを入手する手順と、
前記メッセージの少なくとも一部にアルゴリズムを作用させて得られるＢを生成するためにアルゴリズムを適用する手順と、

ＢとＶを比較する手順と、
ＢとＶが一致した場合に第一の公開鍵と秘密鍵のペアの公開鍵を置き換えの鍵と取り替える手順
とから成ることを特徴とするルート・キーを危機にさらされた状態から回復させる方法。
１１．ルート・キーを危機にさらされた状態から回復させる装置であって、
前記ルート・キーが第一の公開鍵と秘密鍵のペアの秘密鍵であり、
前記装置は、
デジタルプロセッサーと
前記デジタルプロセッサーと接続されていて緊急メッセージを電気的手段により受信する通信インターフェースであって
ルート・キーが危機にさらされたという通知と
置き換えの鍵と危機にさらされたルート・キーを使って生成されたデジタル署名を含んだ緊急メッセージを受信する通信インターフェースと
ルート・キーに対応した公開鍵を保存するメモリと
入力装置であって
緊急メッセージの少なくとも一部にアルゴリズムを作用させて生成されアウト・オブ・バンド・チャネルを通して入手されるＶをデジタルプロセッサーに入力する入力装置とから成り、
前記デジタルプロセッサーは
緊急メッセージのデジタル署名を照合するためにルート・キーに対応した公開鍵を使い

前記緊急メッセージの少なくとも一部にアルゴリズムを作用させて得られるＢを生成するためにアルゴリズムを使い
ＢとＶを比較し
ＢとＶが一致したらルート・キーに対応した公開鍵を置き換えの鍵と取り替えるようにプログラムされている
ことを特徴とするルート・キーを危機にさらされた状態から回復させる装置。

１２．メモリを含むコンピューターで実行可能なコンピュータープログラムを記録したコンピュータ読み取り可能な記録媒体であって、
前記コンピュータプログラムは公開鍵と秘密鍵のペアの秘密鍵であるルート・キーを危機にさらされた状態から回復させるためのプログラムであり
前記記録されたプログラムは、
ルート・キーが危機にさらされたという通知と置き換えの鍵と危機にさらされたルート・キーを使って生成されたデジタル署名を含んだ緊急メッセージをメモリから引き出す処理を前記コンピュータに実行させるコンピュータ読み取り可能な命令と
緊急メッセージのデジタル署名を照合するためにルート・キーに対応した公開鍵を使用する処理を前記コンピュータに実行させるコンピュータ読み取り可能な命令と
緊急メッセージの少なくとも一部にアルゴリズムを作用させて得られるＢを生成するためにアルゴリズムを適用する処理を前記コンピュータに実行させるコンピュータ読み取り可能な命令と
ＢとＶを比較する処理を前記コンピュータに実行させるコンピュータ読み取り可能な命令と
ＢとＶが一致したらルート・キーに対応した公開鍵を置き換えの鍵と取り替える処理を前記コンピュータに実行させるコンピュータ読み取り可能な命令と
から成るプログラムであることを特徴とするメモリを含むコンピュータで実行可能なコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

ルート・キーが危機にさらされた時の回復

背景技術

この発明は、一般的な暗号技術に関し、特にルート・キーが危機にさらされた場合の回復に関する。

暗号技術に関して、公開鍵アルゴリズムと呼ばれる、さまざまなアルゴリズムが開発されてきた。このアルゴリズムは、電子文書の署名や認証に対する非常に有効な手段となる。

一般的に公開鍵アルゴリズムは、公開鍵と秘密鍵と呼ばれる２つの鍵を含んだものである。秘密鍵は、認証機関（certifying authority）によって秘密に保管されている。一方、公開鍵は、その名が示すように公衆に配布される。公開鍵を保持していれば、これを使ってデータを暗号化することが出来るが、この暗号化されたデータは秘密鍵を持った者だけが解読できる。同様に、秘密鍵を持っている者がこれを使って、公開鍵を持った者だけが解読できるような暗号化データを作成することもできる。このように、双方の鍵は共に文書の暗号化に対して有効な手段であり、暗号化された文書は、文書の宛先として指定されていない第三者は読むことが出来ない。

秘密鍵を暗号化に使用した場合、これによって得られた結果をデジタル署名と呼ぶことがある。前記デジタル署名は、秘密鍵を持っている者だけが作り出すことが出来る固有の特徴を持っている。従って、秘密鍵が秘密にされていても、デジタル署名付きの文書を受け取った者は、デジタル署名を照合することによって、この文書の出所を確認することが出来る。デジタル署名の照合は、公開鍵を使ってデジタル署名からデータ列を生成し、このデータ列を前記署名の添付された文書と比較するという、簡単な方法で行われる。前記データ列が添付された文書と同一であれば、受取人は、この文書がまさしく認証機関によって署名された文書であり、この署名された文書の内容は信頼できるということが確信できる。

もちろん、前述の内容は、秘密鍵が実際に秘密に保持されており認証機関だけが知っているということが周知の事実である限りにおいてのみ真実である。秘密

鍵が秘密であるという信頼が失われるや否や、署名が添付された文書を受け取っても、この署名が秘密鍵の信頼を破った者による署名でなく、正しい認証機関による署名であるという確証が得られなくなる。認識機関より上位の、広く信頼されている権威（中央認証機関（central authority）と呼ぶこととする）があれば、鍵の信頼を失った認証機関が新たな秘密鍵を選び、中央認証機関の保証が添付された代わりの鍵を配布することができる。代わりの鍵を受け取った者は、中央認証機関のデジタル署名があるので、新しい公開鍵は新しい秘密鍵に対応したものであることが確信できる。

しかしながら、中央認証機関の秘密鍵の信頼が失われた場合はどうなるのであろうか。また、認識機関より上位の、広く信頼されている権威がなかった場合はどうするのか。それゆえ、公衆が代わりの鍵が正しい鍵でありシステムを破壊しようとしている他者の所有する鍵でないという確証を得るように代わりの鍵をいかに効果的にかつ能率的に配布するか、という問題は、解決が非常に難しい問題である。

発明の開示

この発明の一実施の形態は、一組の公開鍵と秘密鍵の秘密鍵であるルート・キーを置換する方法である。本発明の方法は、ルート・キーを置き換えるという指示、その置き換えられる鍵、及びルート・キーを使って生成されたデジタル署名を含むメッセージを電気的に送信する手順と、通常の通信には用いられないアウト・オブ・バンド・チャネルを使って前記メッセージから導かれる変数Ｖを発行する手順とから成る。置き換えられる鍵は、最初に述べた一組の公開鍵と秘密鍵と置き換えられる別の公開鍵と秘密鍵のペアの公開鍵である。

この発明の最良の形態は、以下に示す特徴を持つ。この発明の方法はまず、メッセージの少なくとも一部分に一方向関数を適用して、変数Ｖを算出する手順を有す。さらに、メッセージ生成時に置き換えの鍵と、メッセージが置き換え鍵の配送であることを示している識別名とを連結する手順を有している。メッセージを生成する手順ではさらに、置き換えの鍵と、（１）どのルート・キーと置き換えを行うのかを特定するシリアル番号と、（２）前記置き換えの鍵の有効期限が終了する期日を示す有効期間終了日と、（３）置き換えの鍵が有効となる期日を

示す有効期間開始日とを、結合する。

この発明のその他の実施の形態もまた、一組の公開鍵と秘密鍵の秘密鍵であるルート・キーを置き換える方法である。その方法は、置き換えの鍵とルート・キーを置き換えられたという指示とを含む第一のメッセージを生成する手順、ルート・キーを使って第一のメッセージからデジタル署名を生成する手順、第一のメッセージとデジタル署名を結合して第二のメッセージを生成する手順、前記第二のメッセージを電気的に送出する手順、アウト・オブ・バンド・チャネルを使って第二のメッセージから得ることが出来る変数Ｖを発行する手順とから成る。

また、この発明のその他の実施の形態は、一組の公開鍵と秘密鍵の秘密鍵であるルートーキーの変更に応ずる方法である。その方法は、ルート・キーが置き換わったことを示すメッセージであって、置き換えの鍵と、ルート・キーを使って生成されたデジタル署名を含むメッセージを電気的に受信する手順と、ルート・キーに対応した公開鍵を使ってメッセージのデジタル署名を照合する手順と、少なくともメッセージのある部分にアルゴリズムを働かせることによってメッセージから算出することのできる変数Ｖをアウト・オブ・チャネルを使って入手する手順と、少なくともメッセージのある部分にアルゴリズムを使って変数Ｂを生成する手順と、ＢとＶを比較する手順と、ＢとＶが一致したならばルート・キーに対応した公開鍵を置き換えの鍵と置き換える手順とから成る。

また、この発明のその他の形態は、ルート・キーが危機にさらされた場合の回復の方法であって、ルート・キーが危機にさらされ信頼を失ったという知らせと共に置き換えの鍵とルート・キーを使って生成されたデジタル署名を含む緊急メッセージを電気的に送信する手順と、緊急メッセージのデジタル署名を照合するために信頼を失ったルート・キーの公開鍵を使う手順と、緊急メッセージの少なくとも一部にアルゴリズムを働かせることによって緊急メッセージから導き出されるＶを、アウト・オブ・チャネルを通して入手する手順と、緊急メッセージにアルゴリズムを働かせてＢを生成する手順と、ＢとＶを比較する手順と、ＢとＶが一致した場合には信頼を失った鍵を置き換えの鍵と取り替える手順とから成る。

また、この発明の他の実施の形態は、ルート・キーが危機にさらされて信頼が

失われた状態からの回復のための装置である。本発明の装置は、デジタル・プロセッサーと、デジタル・プロセッサーと接続していて緊急メッセージを電気信号として受信する通信インターフェースと、ルート・キーに対応した公開鍵を保存しておくメモリと、デジタル・プロセッサーにＶを入力するための入力装置とからなる。前記Ｖは、緊急メッセージの少なくとも一部にアルゴリズムを適用して生成され、アウト・オブ・チャネルを通して入手される。緊急メッセージはルート・キーが危機にさらされ信頼が失われたことを示すと共に、置き換えの鍵と信頼を失った鍵を使って生成されたデジタル署名を含んでいる。デジタル・プロセッサーは、緊急メッセージのデジタル署名を確認するためにルート・キーに対応した公開鍵を使い、Ｂを生成するため緊急メッセージにアルゴリズムを適用し、ＢとＶを比較し、ＢとＶが一致したらルート・キーに対応した公開鍵を置き換えの鍵と取り替えるようにプログラムされている。

また、本発明の他の実施の形態は、ルート・キーを危機にさらされて信頼が失われた状態から回復させるコンピューター・プログラムを記録したコンピュータ読み取り可能な記録媒体である。記録されたプログラムは、コンピューター読み取り可能な次のような命令を有している。（１）コンピューターに、ルート・キーが危機にさらされ信頼を失ったとことを示し、置き換えの鍵と信頼を失ったルート・キーによって生成されたデジタル署名が添付された緊急メッセージをメモリから引き出す処理を行わせ、（２）コンピュータに、緊急メッセージのデジタル署名を照合するため、ルート・キーに対応した公開鍵を使用させ、（３）前記コンピュータに、緊急メッセージにアルゴリズムを適用してＢを生成させ、（４）コンピューターにＢとＶを比較させ、（５）コンピューターに、ＢとＶが等しい場合に、ルート・キーに対応した公開鍵と置き換えの鍵の取り替えを行わせる、手順である。

ルート・キーが危機にさらされた場合の回復は、重大で未解決の問題であって、公開鍵暗号法における悩みとなっている。本発明は、鍵を危機にさらした者によるだまされる危険を冒すことなく、また１００を越える１６進数の桁数を含むような鍵全体を手でシステムに入力する労力を必要とせず、使用者が鍵を電気的

手段により受け取ることが出来るという利点を有する。本発明は、照合用のコードを生成するために一方向関数を用いること、及びすでに利用されているアウト・オブ・バンド・チャネルの存在を利用することによって、わずか１５から２０の１６進数の桁数を再度入力するだけで鍵の取り替えが安全に行える。もっと長い

鍵は電気的手段により受信し、登録することができる。

緊急メッセージに加えてアウト・オブ・バンドによる認証方法を用いることによって、メッセージ及び置き換えの認証用のルート・キーが正当なものであるという強い確信を得ることが出来る。

本発明によれば、中間の存在（例えば、商人）にルート・キーが危機にさらされたことを通知することが出来る。そのため、商人が顧客と何らかの電子情報を送信するとき、この通信に中央認証機関の公開鍵と、使用されているのは新しい公開鍵であるという通知を含む緊急メッセージを添付することが出来る。このように、中央認証機関は、他の存在が緊急メッセージを配布するのをあてにすることができる。さらに、影響のある関係者全てに対して個別に通知を行う責任を持つ必要はない。

その他の利点および特徴は、以下の発明を実施するための最良の形態及び請求の範囲の記載により明らかにする。

図面の簡単な説明

第１図は、緊急メッセージの形式を示した図である。第２図は、ルート・キーを危機にさらされた状態から回復させる処理における中央認証機関の実行処理を示したフローチャートである。第３図は、ルート・キーを危機にさらした状態から回復させる処理における消費者側の実行処理を示したフローチャートである。第４図は、ルート・キーが危機にさらされた場合の回復を実現するコンピュータ・システムのブロック図である。

発明を実施するための最良の形態

緊急メッセージ

この発明は、通常用いられるイン・バンド・チャネルを使って、新しい置き換

え鍵を含むメッセージであって鍵の信頼性が失われたことを示す緊急メッセージを配布する手順と、イン・バンド・チャネルとは異なったアウト・オブ・バンドチャネルを使って、前記メッセージが本物であるかどうかを相手先が確認するための照合コードを発行する手順から成る。イン・バンド・チャネルとは、当事者

間で互いに通常の処理を行うために用いる電気通信路のことを意味する。これには、インターネット、広域ネットワーク（ＷＡＮ）のようなコンピュータ・リンク、電話回線、無線通信等があり、その他多くの可能性がある。アウト・オブ・バンド・チャネルとは、その他の通信路であって、ある特定のエンティティが他のエンティティと通信を行うことのできる通信路を意味する。前記アウト・オブ・チャネルによる通信は、中央認証機関からの一方向の通信だけを行う。これは、新聞の発行と同様なものである。このように、アウト・オブ・バンド・チャネルは、このアウト・オブ・バンドによる通信で受信したものは、中央認証機関であるように見せかけた誰か他の者からのメッセージではなく、中央認証機関からのメッセージであることに関して高い信頼性を有するという特徴を持つ。

図１について説明する。緊急メッセージ１０は、メッセージの識別名１２と、シリアル番号１４と、置き換えの鍵１６と、有効期間開始日１８と、有効期間終了日２０と、デジタル署名２２とから成る。メッセージ識別名１２は、メッセージが緊急メッセージであることを示す。シリアル番号１４は、オプションであり、危機にさらされたルート・キーを特定する識別コードである。中央認証機関が１以上の秘密鍵と公開鍵のペアを使用していた場合には、これを特定することが必要になる。

置き換えられる鍵１６は、新しい公開鍵と秘密鍵のペアの公開鍵であり、前の秘密鍵と公開鍵のペアのルート・キーが信頼を失ったため、その置き換えとして選ばれたものである。

有効期間開始日１８と、有効期間終了日２０を含むデータ・フィールドは、置き換えられた鍵が有効となる期間を示す。有効期間開始日１８は、中央認証機関がシステムの安全性を継続させるプログラムの一部として、公開鍵ー秘密鍵のペアを周期的に変更する手段を有している場合に、特に有効である。このような場

合、中央認証機関は、実際に鍵の変更が行われる前に緊急メッセージを送信し、鍵の使用者が有効期間開始日を経過するまで鍵の変更を行わないようにすることが可能である。そしてもちろん、有効期間終了日２０は、鍵の有効期限が終了する期限を示している。このため、鍵の使用者が誤って古い緊急メッセージを使ってしまうことはない。

最後に、中央認証機関がメッセージに添付したデジタル署名は、信頼を失ったルート・キーを使って生成される。

中央認証機関のプロトコル

図２について説明する。中央認証機関がルート・キーの信頼が失われたと考えられたり、そのような徴候を検出した場合、中央認証機関は新しい置き換えのため公開鍵と秘密鍵のペアを選択し、ユーザに対し置き換えの鍵を配布するための緊急メッセージを作成する（ステップ１００）。置き換えの鍵を含む前記情報を連結して通知情報の一群を生成して、緊急メッセージを作成する。さらに、前記通知情報の一群のためのデジタル署名を作成し（ステップ１０２）、前記通知情報の一群にデジタル署名を添付して緊急メッセージを作成する（ステップ１０４）。

中央認証機関は、信用を喪失したルート・キーをデジタル署名の作成に用いる。この署名を生成する方法は、いくつかある方法のどれでもよい。そのうちのひとつの方法は単に、よく知られているルート・キー使ったデジタル署名アルゴリズムのうちのどれかを採用する方法である。その他の方法としては、まず前記通知情報の一群を一方向関数を用いてより圧縮された表現とし、さらにルート・キーを用いたデジタル署名アルゴリズムを用いる方法がある。

もちろん、後者の方法を用いる場合、緊急メッセージの受け取り側はその認証処理において同じ一方向関数を使わなければならない。このため、一方向関数は公然と入手できるものか、広く知られた一方向関数を想定する。

デジタル署名を添付して完全な緊急メッセージが生成されると、中央認証機関は緊急メッセージを、イン・バンド・チャネルによって同報通信で他の使用者に送信する（ステップ１０６）。イン・バンド・チャネルは、一般的に業務文書の

送受信に使われるものや、一般に利用しやすい通信路である。

中央認証機関はまた、照合コードＶを生成し送信し、この照合コードによって緊急メッセージの受取人は、緊急メッセージが正当なものであるかどうかを確かめる。前記照合コードは、緊急メッセージまたは緊急メッセージの一部に、一方向関数または一方向ハッシュ関数を使って、ハッシュ変数を生成することによって生成される（ステップ１０８）。この一方向関数は、デジタル署名を生成したあるいは生成したと想定される一方向関数と同じであっても、異なっていてもよい。

どちらの場合であっても、中央認証機関は一方向関数ｆ（ｘ）を広く利用できるようにしておく。実際には、完全な一方向関数が存在しないことが知られている。現在一方向関数であると考えられている関数はすべて、最終的にはコンピュータの能力あるいは技術を用いて、与えられたｆ（ｘ１）からｘ１を算出することが十分に可能であろう。従って、一方向関数という語は、ｆ（ｘ１）を知ることによってｘ１を算出することが不可能である必要はないが、算出が非常に難しい関数であるということを意味する。

前述の形態では、ハッシュ関数は、広く知られているＳＨＡ（Secure Hash Algorithm）である。しかしながら、一方向関数は、いくつかの標準的なハッシュ関数（例えば、ＭＤ５、ＳＨＡ、等）のうちのいずかでよい。ＳＨＡやその他条件にあった一方向ハッシュ関数の解説書としては、暗号作成法に関する関する一般的な文献を参照する。例えば、ブルース・シュネイナー（Bruce Schneier）著、アプライド・クリプトグラフィ（Applied Cryptography）、ジョン・ウィリー・アンド・サンズ社（John Wiley &; Sons,Inc.）刊がある。

さらに付け加えると、いくつかの一方向関数を使ったり、これらを結合することが可能であることは言うまでもない。この技術において、多くの一方向関数が知られているが、一般的にその多くは計算が容易であり、このためスマート・カードに装備することもできる。

照合用のコードＶを生成後、中央認証機関はその信頼性を保証するためにコードＶを発行する。すなわちこの方法により、受取人に対して、前記メッセージが

真に中央認証機関からのものであることを保証する（ステップ１１０）。前記方法には、緊急メッセージを送信したチャンネル以外の他の通信チャンネル（すなわち、アウト・オブ・バンド・チャンネル）を使って広くＶを配布することも含まれる。

アウト・オブ・バンド・チャンネルは、ルート・キーを危機にさらした者によって乗っ取られたり、汚染されたりしないことが特に求められる。アウト・オブ・バンド・チャネルは、よく知られた（あるいはコンピューターのアプリケーションの中にハードコードされて変更できないようにした）８００番とするものとする。８００番を用いて鍵の使用者は電話をかけ、ハッシュ変数を照合することができる。あるいは、良く知られた信頼のできる出版物、例えば全国紙や雑誌などであり、照合用の変数を載せて所定の日あるいは期間に所定のページで出版される。鍵の使用者がハッシュ変数を緊急メッセージに作用させて生成した値とアウト・オブ・チャネルを通してハッシュ変数Ｖとを照合することにより、緊急メッセージが正当なものであることに関して高い信頼を得ることが出来る。なぜなら、敵対者が正当な緊急メッセージを提示するためには、アウト・オブ・チャネルを乗っ取ったり、共謀したりしなければならないが、これは全く実現の見込みがないからである。

前述の方法における利点は、緊急メッセージを広く配布することができるということである。中央認証機関は置き換えの鍵を必要としている多くの鍵の使用者全てに対し、即座にアクセスする必要がなくなる。さらに中央認証機関は、緊急メッセージの最初の受取人（例えば商人やベンダー）が、他の鍵の使用者（例えば顧客）に緊急メッセージを伝えるということを信頼することができる。実際に、商人側には緊急メッセージを顧客に広く配布するための動機がある。これは一般的に、中央認証機関の公開鍵は、顧客と商人の間で行われる商取引で取り交わされる情報の認証に必要だからである。

一般使用者のプロトコル

図３について説明する。鍵の使用者は緊急メッセージを、直接中央認証機関からあるいは他の仲介者を介して間接的に電気的手段により受信する（ステップ２

００）。緊急メッセージを受信し、これが緊急メッセージであると認識すると、ユーザはメッセージ中に含まれている有効期間開始日と有効期間終了日を確認し、緊急メッセージが最新のものであることを確認する（ステップ２０２）。メッセージが最新のものであれば、使用者は緊急メッセージの一部であるデジタル署名を確認する（ステップ２０４）。使用者は、これまで使用していた信頼性を喪失したルート・キーを使って公開鍵アルゴリズムによって前記処理を行う。中央認証機関が複数のルート・キーを使っていた場合、緊急メッセージのシリアル番号を調べ、複数の鍵のうち適切なものを確認する。

緊急メッセージが最新のものでありかつ正当なものであることを確認後、アウト・オブ・バンドの情報源から照合用の変数Ｖを入手する（ステップ２０６）。続いて、メッセージの適当な一部分あるいはメッセージ全体に一方向関数を使って変数Ｂを生成し（ステップ２０８）、アウト・オブ・チャネル経由で入手した照合用のＶとＢを比較する（ステップ２１０）。ＢとＶが等しい場合は、緊急メッセージが中央認証機関から送られたものであり、承認を得ないで最初のルート・キーを入手した第三者から送られたものでないという確証が得られる。使用者にとって、Ｂを生成して、これが正しく正当な値であることを確認することが重要である。なぜなら、信頼が失われた鍵では不正実行者がシステムの支配をしようと不正者が緊急メッセージを送信する可能性があるからである。

鍵の使用者がＶとＢが等しいという確証を得た場合は、古い公開鍵を緊急メッセージに含まれている置き換えの鍵と取り替える（ステップ２１２）。この処理実行中にいずれかの箇所でテストに失敗した場合、緊急メッセージを無視し、元のルート・キーに対応する元の公開鍵の使用を続ける。当然ながら、ＶとＢが一致しないと確認された場合、ルート・キーの信頼は失われたが、緊急メッセージはルート・キーを危機にさらした者によるシステムに対する攻撃である可能性が非常に高い。

緊急メッセージに信頼を失ったルート・キーで署名を行うことは、実際に、ルート・キーが信頼を失ったとしても重要な手順であることは明らかである。この署名は、防御のための第一線として働く。システムの正常な働きを中断させて緊

急メッセージを発行することは、誰にでもできることではないことは保証されでいる。署名は、緊急メッセージが二つの発行元のいずれかからのみ発行されたものであることを意味する。すなわち、認証されたルート・キーを持つシステムの認証機関であるか、あるいは、認証されたルート・キーを危機にさらした存在のどちらかである。このように、システムを破壊するため緊急メッセージを使うことの可能な存在の数を大幅に減少させる。

緊急メッセージを処理する手順は、使用者に代わって使用者側のコンピュータ機器（例えばＰＣコンピューター）によって自動的に実行させることができることは明らかである。図４について説明する。コンピューターは一般的に、プログラマブル・デジタル・プロセッサー４００と、緊急メッセージを通信リンク４０３、例えば電話線、経由で受信する通信インターフェース４０２（例えばモデム）を有す。さらに、主メモリと補助メモリを含むメモリ４０４であって、使用者が必要な公開鍵を保存し、緊急メッセージの処理プログラムを含む前記鍵を使うプログラムを保存するためのメモリを有する。前記緊急メッセージの処理プログラムは、コンピューター・ディスク４０８のようなコンピューター読み取り可能な外部媒体からコンピュータ本体にロードされるものとする。また、アウト・オブ・チャネルから引き出した照合コードを入力する入力装置４０６（例えばキーボード）と、関連情報を表示する表示装置（例えばＣＲＴ表示画面）も有する。

コンピューターは通信リンクによって緊急メッセージを受信し、これが緊急メッセージであると認識するようにプログラムされている。このプログラムにより前述した処理が実行される。これらの処理は、完全に自動的に実行されても、使用者に管理や入力を求めても良い。いずれの場合も、メッセージが最新であって正当であるという最初のテスト（すなわち、デジタル署名が信頼を失った鍵によってなされていること）に合格したことを確認することは当然のことである。その後、コンピューターは、新しい鍵の認証のため、照合用コードを入力することを通知する。例えば、画面のダイアログ・ボックスに「ニューヨークタイムズでしかじかの日のｘページに公表されている数を入力してください」、あるいは、

「８００番に電話して読み上げられた番号をタイプしてください」、といった表示がされてもよい。言い換えれば、コンピューターは、指定されたアウト・オブ・チャネル通信により入手した入力（すなわち、照合用の番号あるいは記号列）を要求する。

使用者が入力する照合コードによって緊急メッセージが確認されると、コンピューターはメモリの中の信頼を失った鍵を新しい置き換え用の鍵と取り替える。

例として、ＰＣを用いたが、コンピューター機器は多くの種類のある、デジタル・プロセッサーを有す電子機器であり、例えば、ＰＤＩ、スマート・カード、パームトップ・コンピューター、より強力なワークステイション等があるが、これらはほんの一例に過ぎない。更に付け加えれば、情報の伝達を行うための通信媒体にも多くの可能性がある。例えば、電話線、ケーブル、インターネット、衛星通信、無線通信等である。言い換えれば、本発明は用いられた装置の種類、あるいは採用された通信方法といったことに関して、限定されてしまうことはない。

また、当然のことではあるが、コンピューター機器は、プロトコルを実行するために必要なプログラムとデータが要求するメモリ量全てを、内部あるいは外部のいずれかに持つ。さらに、コンピュータ機器には、その他のコンピューター機器と通信するために必要な機器（例えば、モデム）が含まれる。付け加えれば、情報の伝達を行うための通信媒体にも多くの可能性がある。例えば、電話線、ケーブル、インターネット、衛星通信、無線通信等である。言い換えれば、本発明は用いられた装置の種類、あるいは採用された通信方法といったことに関して、限定されてしまうことはない。

その他の例は、以下の請求の範囲で述べる。

【図１】

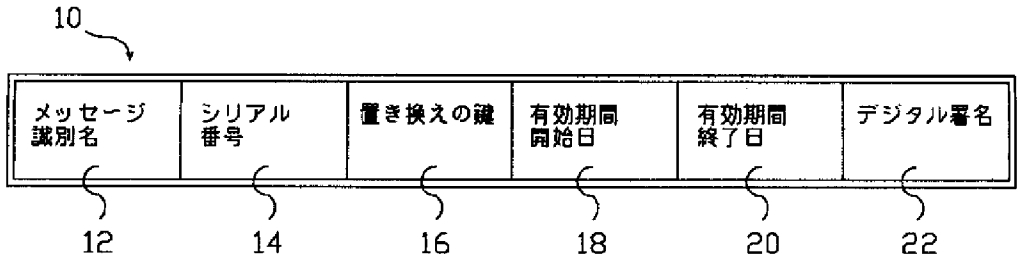
10
メッセージ識別名
シリアル番号
置き換えの鍵
有効期間開始日
有効期間終了日
デジタル署名
12
14
16
18
20
22

図1

【図２】

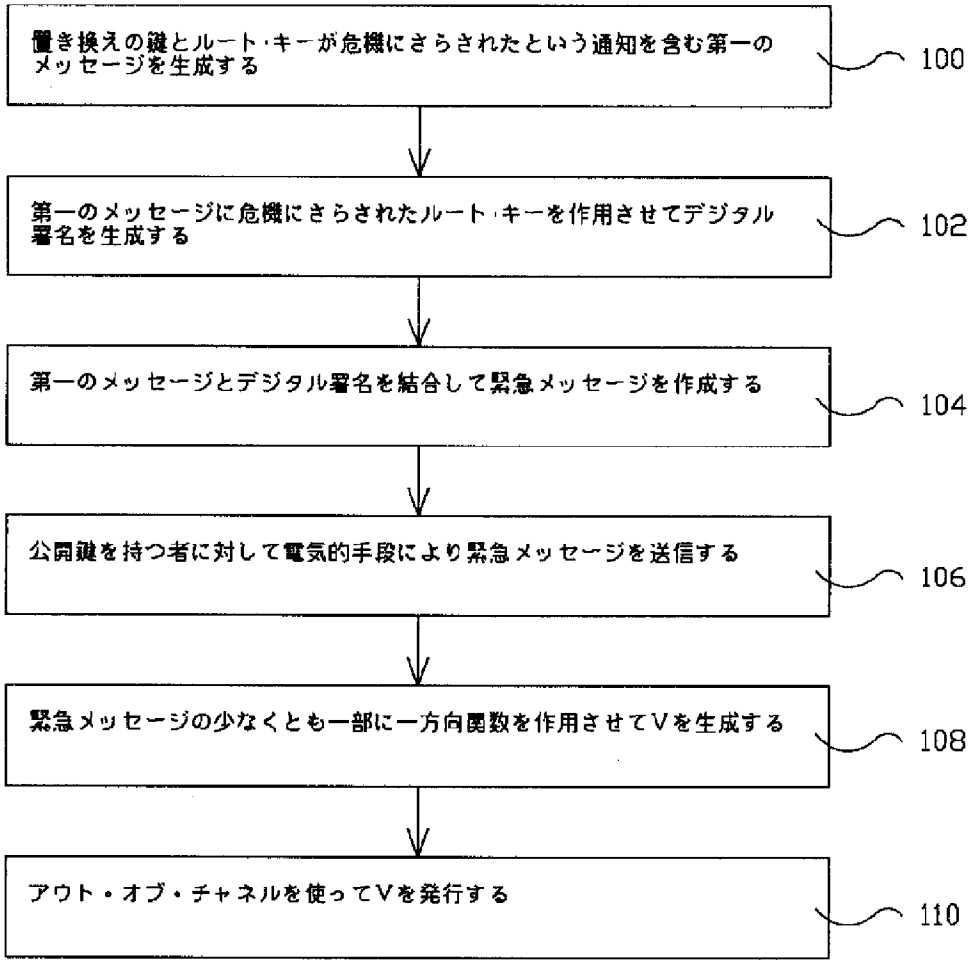
置き換えの鍵とルート・キーが危機にさらされたという通知を含む第一のメッセージを生成する
100
第一のメッセージに危機にさらされたルート・キーを作用させてデジタル署名を生成する
102
第一のメッセージとデジタル署名を結合して緊急メッセージを作成する
104
公開鍵を持つ者に対して電気的手段により緊急メッセージを送信する
106
緊急メッセージの少なくとも一部に一方向関数を作用させてＶを生成する
108
アウト・オブ・チャネルを使ってＶを発行する
110

図2

【図３】

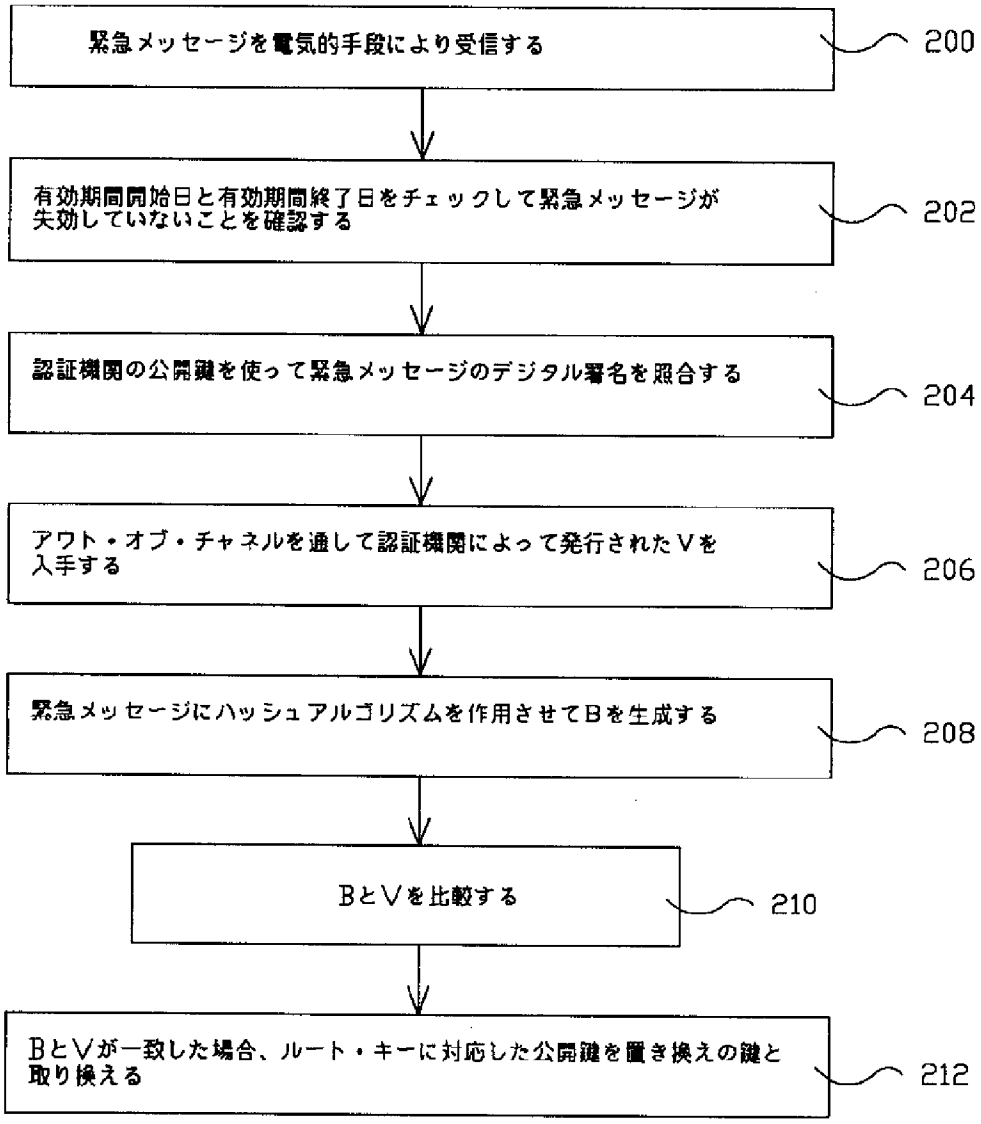
緊急メッセージを電気的手段により受信する
200
有効期間開始日と有効期間終了日をチェックして緊急メッセージが失効していないことを確認する
202
認証機関の公開鍵を使って緊急メッセージのデジタル署名を照合する
204
アワト・オブ・チャネルを通して認証機関によって発行されたＶを入手する
206
緊急メッセージにハッシュアルゴリズムを作用させてＢを生成する
208
ＢとＶを比較する
210
ＢとＶが一致した場合、ルート・キーに対応した公開鍵を置き換えの鍵と取り換える
212

図3

【図４】

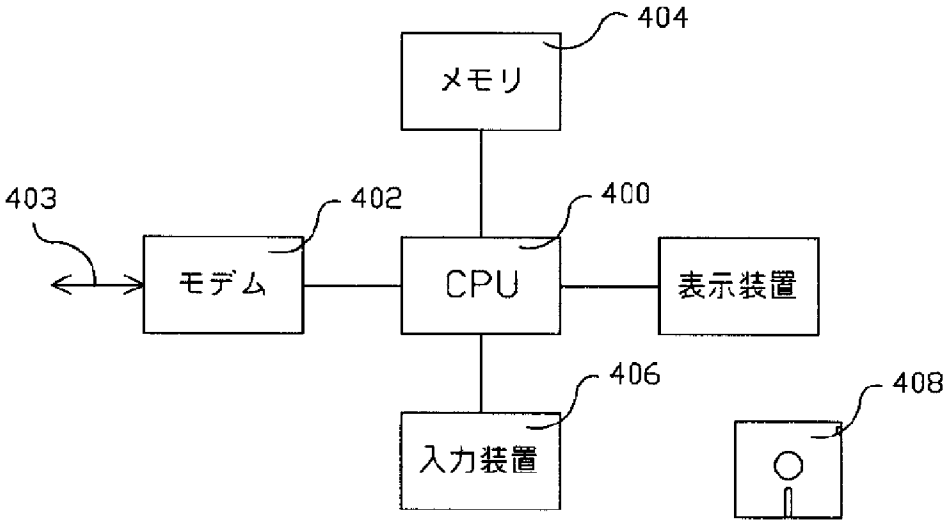

図4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/18037

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H04L 9/08
US CL : 380/21, 30, 49

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/21,30,48,49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS terms: key replace, key update, digital signature, certification, certifying certificate,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,799,258 A (DAVIES) 17 January 1989.	1-10
A,P	US 5,469,507 A (CANETTI ET AL.) 21 November 1995; Figures 2 and 3; column 5 lines 55-66; claims 1 and 2.	1-3, 7-12
A,P	US 5,499,294 A (FRIEDMAN) 12 March 1996, Figures 2 and 3C.	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 04 MARCH 1997	Date of mailing of the international search report 08 APR 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PINCHUS M. LAUFER Telephone No. (703) 306-4160

Form PCT/ISA/210 (second sheet)(July 1992)*